



Contingency Software in Autonomous Systems

*NASA OSMA Software Assurance Symposium
July 18-20 , 2006*



Robyn Lutz, JPL/Caltech & ISU
Ann Patterson-Hine, NASA Ames

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, and at NASA Ames Research Center, under a contract with the National Aeronautics and Space Administration. The work was sponsored by the NASA Office of Safety and Mission Assurance under the Software Assurance Research Program led by the NASA Software IV&V Facility. This activity is managed locally at JPL through the Assurance and Technology Program Office



Contingency Software in Autonomous Systems

Problem



PROBLEM STATEMENT

Autonomous vehicles currently have a limited capacity to diagnose and mitigate failures.
We need to be able to handle a *broader* range of contingencies (anomalous situations).

GOALS

1. Speed up diagnosis and mitigation of anomalous situations.
2. Automatically handle contingencies, not just failures.
3. Enable projects to select a degree of autonomy consistent with their needs and to incrementally introduce more autonomy.
4. Augment on-board fault protection with verified contingency scripts



Contingency Software in Autonomous Systems

Approach



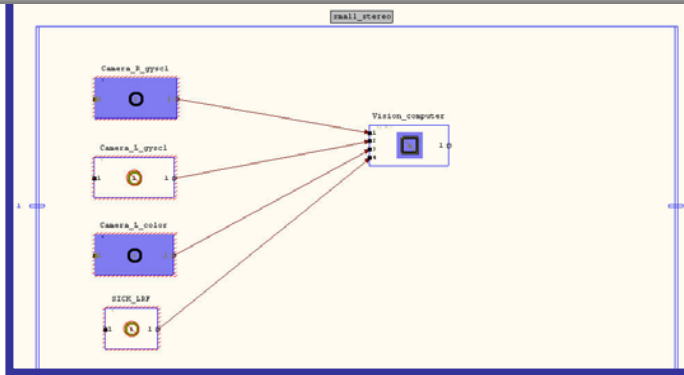
1. ***Identify contingencies*** that risk mission-critical functions in a power system testbed (using S-FTA, S-FMECA, Obstacle Analysis)
2. ***Model contingencies*** & autonomous recovery actions using TEAMS (Testability And Engineering Maintenance System, QSI)
3. ***Analyze contingencies***: TEAMS produces diagnostic tree of checks needed to detect & isolate contingency, identifies missing checks and recovery actions
4. ***Code contingencies'*** diagnosis & recovery behavior in the project's planner scripting language (auto-translation from TEAM's XML output)
5. ***Verify contingency scripts*** with hardware-in-loop simulation

Using the above steps,

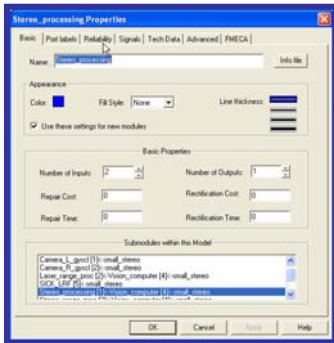
- Verify contingency plans used by NASA projects
- Investigate issues in coverage of contingencies
- Test results on power system testbed



Contingency Software in Autonomous Systems Approach



1. TEAMS Model



3. XML auto-translated
to verify contingency
handling on platform

testRightCameraNotTooDark

Test:

testRightCameraNotTooDark

```
</LABEL>
<SYMPTOM />
<NODE LABEL="1"
TYPE="TEST"
ID="T.small_stereo_0.1.2.
4.0" PASS="YES"
FAIL="NO">
<PARA>
- <![CDATA[
```

testRightCameraNotTooBright

Test:

testRightCameraNotTooBright

Open Right Lens Cap

testLeftCameraNotTooDark

Test:

testLeftCameraNotTooDark

Desaturate Right Camera

2. Diagnostic Tree
auto-generated

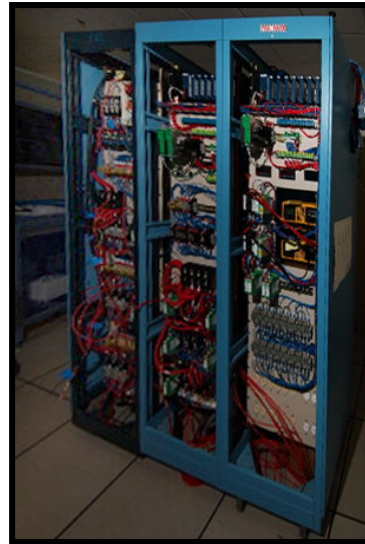


Contingency Software in Autonomous Systems

Relevance to NASA



ARC



ARC



JPL

- Improved contingency handling needed to safely relinquish control of unpiloted vehicles to autonomous controllers
- More autonomous contingency handling needed to support extended mission operations



Contingency Software in Autonomous Systems



Accomplishments

- Completed Autonomous Rotorcraft Project case study
 - **Documented process & results (1 published & 2 submitted papers)**
 - **Performed hardware-in-loop testing of diagnostic tree**
 - **Project applied results, modifying camera controller to enable autonomous switching between color and video cameras**
- Modeled MER Critical Pointing software to be reused on MSL
 - **Called if commandability lost; before trajectory-correction maneuvers**
 - **Auto-generated diagnostic tree from TEAMS model of what is known when a “quit-failed” signal occurs**
 - **Supplemented available documentation**
- New case study
 - **ADAPT emulates a typical spacecraft power system with redundant power buses, a solar panel, and battery storage**
 - **The approach for developing contingencies resulted in critical function identification and preliminary identification of required contingency plans**
- Described work at Mini-SAS at JPL



Contingency Software in Autonomous Systems

Tech Transfer Potential



1. Contingency management of complex systems is essential to the **robust** operation of complex systems such as spacecraft, Unpiloted Aerial Vehicles (UAVs) and vehicles for Exploration missions
2. Automatic contingency handling allows a **faster** response to unsafe scenarios, with reduced human intervention
3. Results, applied to the Advanced Diagnostics and Prognostics Testbed, the Autonomous Rotorcraft Project UAV, and Mars Science Lab, pave the way to more resilient, adaptive **autonomous** systems



Contingency Software in Autonomous Systems

Next Steps



- Investigate and model with TEAMS key contingencies involved in safe software reconfiguration of power distribution systems to support autonomous operations
- Demonstrate and verify a subset of the contingency responses we have developed on available platforms
- Document process to encourage transfer to other NASA projects